The Avenger

Usage and Release Notes

The Avenger is a full-scriptable, kernel-level driver designed to remove highly persistent files and registry keys/values protected by entrenched malware. Basically this means that The Avenger is a program to which you give commands to execute (the *script*) consisting of files to delete, etc., which would otherwise be hard to delete because they were protected or "in use" by malicious software. With the recent proliferation of rootkits and other strongly-protected forms of malware, a tool like this one to remove deeply-entrenched files has become more and more necessary.

The Avenger is currently at version 1.

Every attempt has been made to ensure its safety, but it is provided with absolutely no warranty whatsoever and its safety cannot be 100% guaranteed! You use The Avenger at your own risk – please use it only under qualified supervision. For assistance please contact me at Swandog46 [at] mvps [dot] org , or one of the helpers at one of the ASAP forums, such as SWI.

Be forewarned! – The Avenger is a VERY powerful program, designed to remove highly persistent files and registry keys. As a result, it can easily be misused. **Certain misuses of this program could prevent your system from ever starting up again.** Please be careful!

Usage and release notes for The Avenger are listed below, in four sections:

(1) System requirements and program usage
(2) Script syntax
(3) Command line arguments and usage
(4) License, credits, and acknowledgements

(1) System Requirements and Program Usage

System Requirements:

1) The Avenger will work ONLY on Windows 2000 and XP, and only on 32-bit versions! Please do NOT attempt to use it on any other operating system. It has not been tested on 64-bit platforms.
2) The Avenger must be run from a user account with administrator privileges.

Program Usage:

The Avenger may be downloaded from here , or from my main tools page.

When run, the main Avenger window allows you to choose from one of three options for inputting a script to execute: (1) load a script from a file, (2) load a script from an internet URL, or (3) input a script manually. Clicking the Open File button or going to the File menu and choosing "Open script file..." will allow you to

load a script from a file. Typing a URL into the "Load script from Internet URL" field will allow you to load a script from a URL (please note that you must include the http:// prefix when loading scripts from URLs!). Selecting "Input script manually" and then clicking the magnifying glass icon: will allow you to type script commands directly for execution. If "Load script from file" or "Load script from URL" is selected, clicking the magnifying glass icon will allow you to view the current script in memory and edit it if desired.

Clicking the "green light" icon: will begin execution of the script currently in memory.
Clicking the "stop" icon: will quit the program.

The log from the most recent use of The Avenger may be viewed by going to the File menu, and choosing "Open log file." Finally, help and version information is available from the Help menu.

After you have clicked on the "green light" to begin execution of a script, The Avenger will set itself up to run the next time you reboot your computer, and then will prompt you to restart immediately. After your system restarts, a log file should open with the results of Avenger's actions. This log file is located at %systemdrive%\avenger.txt, where %systemdrive% is a variable representing the main system drive of your computer (usually C:\ for most systems). The Avenger will also have backed up all the files, etc., that you asked it to delete, and will have zipped them and moved the zip archive to %systemdrive%\avenger\backup.zip. Registry backups will be inside this archive under the name backup.reg.

(2) Script Syntax

The core of The Avenger is its script-processing functionality. As a result, I must discuss the syntax used in Avenger scripts. An Avenger script is composed of lines of plain text, containing one command directive per line. There are 11 commands in total that The Avenger recognizes. They are:

1) Comment:
2) Files to delete:
3) Files to replace with dummy:
4) Files to move:
5) Folders to delete:
6) Registry keys to delete:
7) Registry keys to replace with dummy:
8) Registry values to delete:
9) Registry values to replace with dummy:
10) Programs to launch on reboot:
11) Drivers to unload:

Blank lines and whitespace in general including leading and trailing whitespace on command lines is ignored by The Avenger. (If you do not want whitespace to be stripped, you may enclose parts or all of any commands in quotation marks "", which will override whitespace stripping.) All commands are case-insensitive.

The commands, respectively, do the following:

1) Comment: does nothing. Comment lines are so that

script-writers can put comments into their scripts.

2) Files to delete: deletes and backs up files listed (NOTE: this works only on files, not folders)

3) Files to replace with dummy: replaces files listed with empty "dummy" files, and backs up originals.

4) Files to move: moves files from a source location to a destination, backing up any existing destination files. This command will only work within drives/volumes (for example, do not try to move a file from D:\ to C:\ ; it will not work.)

5) Folders to delete: deletes and backs up folders listed (NOTE: this works only on folders, not files.)

6) Registry keys to delete: deletes and backs up registry keys listed. HKEY_LOCAL_MACHINE and HKEY_USERS are the only recognized registry hives, and either these long names or the abbreviations HKLM and HKU are acceptable.

7) Registry keys to replace with dummy: replaces all values under the selected registry key (recursively) with dummy values – that means null strings for string values, and 0 for numeric values.

8) Registry values to delete: deletes and backs up specific registry values under registry keys as above.

9) Registry values to replace with dummy: replaces a single value under a registry key with a dummy as above.

10) Programs to launch on reboot: queues a program to run once at next reboot, to be able to extend Avenger to simple user-mode code and incorporate "cleanup" steps or larger malware fixes.

11) Drivers to unload: this is an experimental command, and should please be used sparingly. It will unload other system drivers, including kernel- and boot-level drivers. This process

requires TWO reboots, which will be automatically queued if any drivers to unload are listed. Please note that driver FILES are NOT automatically removed by this command. If you want files deleted in addition, you will have to add that yourself as a separate files to delete: command.

One other important note: environmental variables such as %systemdrive%, %windir%, %temp%, or any other variable recognized by the command interpreter (including user-defined variables such as in a batch script) may be used in any Files commands (Files to delete: , Files to Replace with Dummy: , Files to move: , or also in Folders to delete: and Programs to launch on reboot:).

Because I know all of this is quite abstract, here is a concrete example of a functional script file:

```
comment:
I didn't really need to put in the comment: line since all
leading lines not matching a command directive are interpreted
as comments.
But it is just to illustrate how comments work.
After reading the Comment:  directive above, The Avenger will
ignore all subsequent lines until it finds another command
directive.  Please remember to put the colons :  in when you put
in command directives!  Now I will add real commands so you can
see sample syntax for each one.

Files to delete:
c:\windows\system32\badfile.dll
%windir%\system32\badfile2.dll
%systemdrive%\somefile.ext
```

Comment:
Note the syntax of one file per line listed after the files to delete: command. Also note the use of environmental variables in the file names themselves.

Files to replace with dummy:
D:\somefile.ext

FILES TO MOVE:
C:\SOMESOURCEFILE | c:\somedestinationfile
"C:\SOMESOURCEFILE" | "c:\somedestinationfile"

Comment:
Note the case insensitivity of the commands. Also note the syntax of the files to move: command, using the pipe | to separate the source and destination paths. Whitespace is stripped before and after the pipe, up to any quotes "" that are found.

Folders to Delete:
C:\somefolder

registry keys to delete:
hklm\software\badkey
hkey_local_machine\system\currentcontrolset\somebadkey

registry keys to replace with dummy:
hku\.default\somebadkey
hklm\software\some long key name

Comment:
note that HKLM and HKU as well as HKEY_LOCAL_MACHINE and HKEY_USERS are accepted (case-insensitive as always). Also note that some long key name is a perfectly valid key name, and will be recognized since only leading and trailing whitespace is stripped (although if you are ever uncertain you can always add

```
quotes “”).


registry values to delete:
HKEY_USERS\.default\badkey | somebadvalue

COMMENT:
Note the use of the pipe | syntax again to separate registry key
names from registry value names in the registry values to
delete:  command.

Registry values to replace with dummy:
HKLM\SomeKeyPath\Blah\Blah|somevalue


programs to launch on reboot:
%systemdrive%\mybatch.bat



drivers to unload:
BadServiceName

COMMENT:
The syntax for drivers to unload:  is just to list the Service
name of any driver you want unloaded.  This would be the Service
Name, as opposed to the Display Name usually visible in services.
msc.  The Service name is also the name of the subkey under HKLM
\System\CurrentControlSet\Services.
```

This is a valid script file. As another example without the cluttering comments, here is a similar script file, but greatly simplified.

```
Files to delete:
C:\test.txt

Registry keys to delete:
HKLM\Software\Test
```

Give it a try! This sample script file is uploaded at http://swandog46.geekstogo.com/samplescript.txt. Create a fake file called c:\test.txt, and a fake registry key called HKEY_LOCAL_MACHINE\Software\Test, and then download and run The Avenger. Select "Load script from Internet URL", and in the address bar paste the URL http://swandog46.geekstogo.com/samplescript.txt. Then click the "green light" icon, and reboot, and watch what happens! C:\test.txt will be deleted and backed up to C:\Avenger, as will HKLM\Software\Test. The entire process will be logged to C:\avenger.txt (assuming your %systemdrive% is C:\ ).

(3) Command Line Arguments and Usage

The Avenger may be run with full functionality from the command line, and the GUI may be completely suppressed in order for Avenger to be combined into larger scripts and malware fixes. If the "/nogui" flag is specified on the command line the GUI will be suppressed, and then other command line arguments will be checked. (All other command line arguments are ignored if "/nogui" is not specified.) The command line flags are:

/nogui – suppresses GUI.
/q – Quiet Mode. Suppresses warnings and informational messages, but not errors

/qq – Silent Mode. Suppresses all messages except for fatal errors that require termination. Please use this flag sparingly since it suppresses some nonfatal errors that you should otherwise know about!
/r – Reboot Automatically. Ignored if not Silent Mode. Reboots automatically after setup, without prompting user first.
/s *ScriptLocation* – redirect script. Avenger will look for the script to load at *ScriptLocation*. This may either be a file path or a web URL (if a web URL it must contain a prefix "http://" to let the program know). You may also enclose paths in quotes "" if there is any concern about spacing. If this flag is not set, Avenger looks for a script file at **script.txt** in the current working directory. If set, /s should be the last flag on the command line.

So the full command line usage is:

avenger.exe /nogui [/q] [/qq [/r]] [/s *ScriptLocation***]**

When The Avenger is run from the command line, it will return a 1 to the environment if it fails, and a 0 if it succeeds (Unix style). I think (although I haven't tested it) that you could test for its success by using IF NOT ERRORLEVEL 1 in a batch.

(4) License, Credits, and Acknowledgements

Permission is granted to use The Avenger freely for non-commercial purposes, but insofar as I have the legal right to do so, **I insist please that The Avenger not be incorporated into other software, hosted, mirrored, or otherwise**

redistributed in any way without my express permission. Please see my main tools page for more information.

In addition, **by using The Avenger you agree that you do so at your own risk, with full knowledge that I provide absolutely no warranty whatsoever or guarantee of the program's safety.**

Thank you very much to everyone who provided me feedback and helped in beta testing. I know that I will not be able to list every single person here, and if I missed you I apologize, and thank you too! But I wish to express the greatest gratitude to miekiemoes, IMM, Assarbad, LonnyRJones, Mosaic1, Grinler, Nigel, jedi, and many others.

I would also like to acknowledge that I utilize the Info-ZIP compression software in this program, and as per their licensing requirements, below are the full contents of the Info-ZIP license:

This is version 2005-Feb-10 of the Info-ZIP copyright and license. The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Please note that my adherence to the Info-ZIP licensing requirements IN NO WAY implies that anyone may redistribute The Avenger in similar fashion. Any and all redistributions of The Avenger are STRICTLY PROHIBITED as discussed above.

Please report any bugs or comments, good or bad, to me at Swandog46 [at] mvps [dot] org. Enjoy The Avenger!

Back to Tools Home